Retrouvrer les traces d’une attaque informatique peut s’avérer complexe et coûteuse

Retrouvrer les traces d’une attaque informatique peut s’avérer complexe et coûteuse

Selon l'un des principes fondamentaux de la police scientifique, sur une scène de crime, tout contact laisse une trace. Dans l'univers de la cybercriminalité, chercher les traces pour remonter le fil des événements jusqu'à l'auteur de l'attaque, se révèle souvent compliqué.

Lorsqu'un incident survient, il est généralement difficile pour l'entreprise de définir qui a accédé à son système d'information et ce que cette personne – ou groupe de personnes – a fait. La tâche se complique encore un peu plus lorsque cet incident provient d'utilisateurs internes bénéficiant d'un haut niveau de privilèges sur le système – voire même de la personne en charge de prévenir les attaques sur le réseau.
Que l'incident soit le résultat d'une action malveillante d'un utilisateur interne, d'une erreur humaine ou d'une faille, dès lors que l'entreprise n'est pas capable de remonter les informations, elle passe à côté de preuves cruciales, et rend l'enquête beaucoup plus longue et onéreuse.

Le facteur temps : la clé de la réussite
Dans toutes investigations post-incident de sécurité, le temps est un facteur crucial. Pour mener à bien une enquête, il est plus facile, plus précis et généralement moins couteux de conduire une analyse criminalistique, dite forensics, poussée immédiatement, plutôt que plusieurs semaines voire plusieurs mois après l'incident.
L'examen approfondi des logs : remonter les étapes d'une attaque
Lorsqu'une faille est avérée, l'entreprise dépend des logs générés par les terminaux et les applications sur le réseau, pour déterminer la cause initiale et remonter les étapes de l'attaque. En pratique, trier les informations peut prendre des jours – en d'autres termes, cela revient à chercher une aiguille dans une botte de foin.
L'intégrité des logs : le respect du standard des preuves
Si les logs ont été modifiés et qu'ils ne peuvent pas être présentés dans leur format original, l'intégrité des données de logs peut être remise en question lors d'une procédure légale. Les logs doivent respecter le standard légal des preuves, en étant collectés de manière inviolable. A contrario, les logs qui ont été modifiés ou qui n'ont pas été stockés de manière sécurisée, ne seront pas acceptés comme preuve légale dans une cour de justice.
Cependant, même pour les organisations qui ont implémenté des solutions fiables de collecte et de gestion des logs, l'information cruciale peut manquer et ce chainon manquant peut empêcher l'entreprise de reconstituer tout le cheminement de l'incident et ainsi de retrouver la source initiale du problème.

Les comptes à privilèges : une cible fructueuse pour les cybercriminels
En ciblant les administrateurs du réseau et autres comptes à privilèges qui disposent de droits d'accès étendus, voire sans aucune restriction au système d'information, aux bases de données, et aux couches applicatives, les cybercriminels s'octroient le pouvoir de détruire, de manipuler ou de voler les données les plus sensibles de l'entreprise (financières, clients, personnelles, etc.).

L'analyse comportementale : un rempart nouveau pour les entreprises
Les nouvelles approches de sécurité basées sur la surveillance des utilisateurs et l'analyse comportementale permettent aux entreprises d'analyser l'activité de chacun des utilisateurs, et notamment les événements malveillants, dans l'intégralité du réseau étendu.
Ces nouvelles technologies permettent aux entreprises de tracer et de visualiser l'activité des utilisateurs en temps réel pour comprendre ce qu'il se passe sur leur réseau. Si l'entreprise est victime d'une coupure informatique imprévue, d'une fuite de données ou encore d'une manipulation malveillante de base de données, les circonstances de l'événement sont immédiatement disponibles dans le journal d'audit, et la cause de l'incident peut être identifiée rapidement.
Ces journaux d'audit, lorsqu'ils sont horodatés, chiffrés et signés, fournissent non seulement des preuves recevables légalement dans le cadre d'une procédure judiciaire, mais ils assurent à l'entreprise la possibilité d'identifier la cause d'un incident grâce à l'analyse des données de logs.
Lorsque ces journaux sont complétés par de l'analyse comportementale, cela offre à l'entreprise une capacité à mener des investigations forensics beaucoup plus rapidement et à moindre coût, tout en répondant pro activement aux dernières menaces en temps réel… [Lire la suite]

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet…) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Source : *Recouvrer les traces d'une attaque informatique : l'investigation peut s'avérer complexe et coûteuse – JDN*

Top 10 des arnaques sur Facebook en 2014

Top 10 des arnaques sur Facebook en 2014

Une étude des analystes antivirus Bitdefender révèle que Taylor Swift n'est plus aussi populaire que l'année dernière, lorsqu'une fausse vidéo à son sujet avait permis de répandre massivement un malware sur le réseau social. Chaque année, des millions d'utilisateurs tombent dans les pièges des arnaques diffusées sur Facebook. Voici le classement des 10 arnaques les plus répandues dans le monde, depuis le début de l'année 2014 !

1. **Qui a visité mon profil**– 30.20% (anglais – international)
2. **Changez la couleur de votre Facebook** – 7.38% (anglais – international)
3. **La sextape de Rihanna avec « son » petit-ami**– 4.76% (anglais – international)
4. **Consultez mon nouveau statut pour recevoir gratuitement un T-shirt officiel Facebook** – 4.21% (anglais – international)
5. **Dites au revoir au Facebook bleu**– 2.76% (français)
6. **Produits défilmés. Distribution gratuite**– 2.41% (anglais – international)
7. **Vérifiez si un ami vous a supprimé de sa liste** – 2.27% (anglais – international)
8. **Cliquez ici pour voir le top 10 des profils qui vous harcèlent le plus ! Vous serez étonné d'apprendre que votre ex visite toujours votre profil !** – 1.74% (anglais – international)
9. **Découvre comment voir qui visite ton profil, tu n'es pas au bout de tes surprises !** – 1.55% (espagnol)
10. **Je viens de modifier le thème de mon Facebook. C'est incroyable**– 1.50% (anglais – international)

Autres : 41.22%

Alors que Taylor Swift quitte le Top 10, **Rihanna reste la star la plus utilisée en tant qu'« appât »** par les scammers pour répandre un malware via Facebook.
L'arnaque des billets "gratuits" pour Disneyland sort aussi du classement alors qu'en juillet dernier, elle surclassait l'arnaque « Je peux vérifier qui regarde mon profil » qui avait fait des dizaines de milliers de victimes. Le scam « **Qui a visité mon profil » conserve quant à lui sa 1ère place**, représentant presque un tiers de la part totale des arnaques sur Facebook (30.20%).
Les arnaques du type « changez la couleur de votre Facebook » se sont internationalisées et représentent dorénavant **7,38 % de la part totale des scams sur Facebook** (vs 4.16% en 2013).

Les mêmes arnaques Facebook fonctionnent toujours

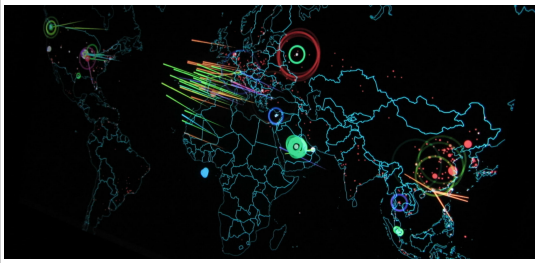
« Pourquoi les utilisateurs veulent-ils toujours savoir qui a jeté un coup d'œil à leur profil, malgré tous les avertissements de sécurité à ce sujet ? » déclare Catalin Cosoi, Responsable de la Stratégie de sécurité chez Bitdefender. *« Ils pensent certainement qu'il s'agit de vraies applications… C'est ce que l'on appelle de l'ingénierie sociale, et elle atteint alors son plus haut niveau – un jeu psychologique entre le cybercriminel et sa victime. Les appâts ont changé avec le temps – harceleurs, voyeurs, admirateurs, petites amies trop attachées et ex qui vous hantent, mais la raison pour laquelle ces arnaques fonctionnent est simple : la nature humaine. »*
Une offre de **T-shirts Facebook gratuits** fait son entrée dans le Top 10 (4.21 %). Les fans intéressés par des vêtements à l'effigie de la marque américaine se retrouvent à remplir de **fausses études ou à installer des add-ons malveillants** qui exploitent leurs données personnelles.
L'autre nouveauté de ce classement concerne des arnaques qui piègent les utilisateurs avec des **cadeaux publicitaires défilmés** (2,41 %).
Au cours de ces deux dernières années, les **arnaques sur Facebook se sont multipliées** en même temps que la plate-forme de réseau social s'est développée. L'étude Bitdefender montre aussi une augmentation du nombre d'arnaques via des **vidéos virales qui utilisent de façon abusive les *"Like"*** Facebook et les options de partage. L'année passée, les sites frauduleux utilisant le **likejacking** (détournement de « *J'aime*«), **clickjacking** (détournement de liens) et **YouTube** ont proliféré en anglais mais aussi en allemand, chinois et en italien.
Pour éviter d'être détectés plus facilement, les scammers peuvent utiliser des caractères spéciaux et numéros dans la description de leur fausse application. Une **variante populaire du scam « Top profil visiteurs »** attire de nouvelles victimes avec ce message : *"Check 0ut n0w wh0 viewed ur profile"*.
Cette étude se base sur les données issues de l'outil Safego de Bitdefender, l'application Facebook gratuite qui scanne les timelines et alerte les utilisateurs en cas de posts malveillants et frauduleux. Pour plus d'informations sur la protection de vos comptes utilisateurs de médias sociaux, vous pouvez consulter le guide de sécurité de Bitdefender à ce sujet… [Lire la suite]

Source : *Fausses sextapes et arnaques diverses : le top 10 des scams en 2014 sur Facebook*

A quoi doit-on s'attendre en matière de cybersécurité à l'horizon 2020 ?

A quoi doit-on s'attendre en matière de cybersécurité à l'horizon 2020 ?

A l'heure où les objets connectés continuent de se déployer et où les piratages de données personnelles ou professionnelles se multiplient, quel avenir peut-on envisager en termes de cybersécurité ? Un groupe de chercheurs a élaboré plusieurs scénarios.



Le Centre pour la cybersécurité à long terme, un groupe de chercheurs pluridisciplinaires de l'Université de Berkeley en Californie, s'est questionné sur ce possible avenir en fonction de divers paramètres (déploiement de l'IoT, avancées technologiques, initiatives politiques, etc.). Et selon eux, plusieurs scénarios émergent :

• The New Normal décrit un monde où les cyberattaques à grande ou petite échelle seront, en 2020, autant légion que personnelles, dépassant les pouvoirs publics par leur nombre et leur ampleur, et encombrant les cours de justice de dossiers liés à la criminalité digitale – une sorte de « Far West 2.0 » dans lequel les utilisateurs n'hésiteraient pas à se rendre justice par eux-mêmes ;

• Omega conte, quant à lui, le futur de l'analyse prédictive : bien au-delà des études démographiques, la nouvelle génération d'algorithmes pourrait cibler plus étroitement les caractéristiques et préférences d'un individu donné, ce qui pourrait introduire un débat des plus clivants, à la frontière du philosophique et du politique, sur la manipulation comportementale ;

• Sensorium, enfin, dépeint l'évolution du *quantified self* jusqu'à faire d'Internet un vaste système de « lecteurs d'émotions », comme le souligne The Conversation, touchant du doigt les aspects les plus intimes de la psychologie humaine. Au risque que les données des applications de *quantified self* émotionnelles puissent être « retournées » contre leurs utilisateurs.

Plus d'informations et plus de scénarios ici.

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Source : *Quel avenir pour la cybersécurité à l'horizon 2020 ?* |

Denis JACOPINI participera au 8e IT-Forum à Abidjan les 2 et 3 juin 2016

Denis JACOPINI participera au 8e IT-Forum à Abidjan les 2 et 3 juin 2016

La 8e édition du IT-Forum (Forum des décideurs et acteurs des Technologies de l'Information) se déroulera les 2 et 3 juin prochain à Abidjan.

IT FORUM 8ème EDITION

Des conférences seront animées en plénières par des spécialistes, des Experts-Consultants et des Universitaires. Ce sera le lieu de faire des exposés, de partager des expériences, de former et d'informer les participants.
Les enjeux de la transformation numérique et plus globalement de l'appropriation des nouvelles technologies modifient considérablement notre mode de vie. La sécurisation des données et des dispositifs de paiement comporte des failles qu'il comporte d'améliorer pour apporter la confiance nécessaire au climat des affaires.
De nombreuses études viennent conforter ce constat et tendent à démontrer le potentiel de croissance du secteur.
En Côte d'Ivoire, les transactions mobiles s'élèvent à 15 milliards de FCFA par jour soit 22,5 millions d'Euros.
Des montants qui donnent le vertige et qui poussent les sites marchands notamment les opérateurs de télécommunications à prendre des mesures de sécurité de plus en plus importantes… mais qui montrent aussi rapidement leurs limites !
Au fil des années, la Côte d'Ivoire s'est imposée comme l'un des leaders naturels dans le domaine des transactions mobiles en Afrique.
En insistant sur la priorité à donner à la protection des données et des transactions (mobile banking, eCommerce),
Devenu un rendez-vous incontournable depuis une décennie, l'IT Forum s'impose aujourd'hui comme l'une des
rencontres les plus importantes.
QUAND
Jeudi 2 juin 2016 à 08:00 – Vendredi 3 juin 2016 à 18:00 (Heure : Côte d'Ivoire) – Ajouter au calendrier
LIEU
Maison de l'entreprise – CGECI (Confédération Générale des Entreprises de Côte d'Ivoire – Patronat ivoirien), Avenue Lamblin, Abidjan, Lagunes, Côte d'Ivoire, Abidjan, Plateau, Cote d'Ivoire –
PROGRAMME
http://www.ciomag-event.com/8eme-edition-it-forum-cote-d-ivoire

---

Réagissez à cet article

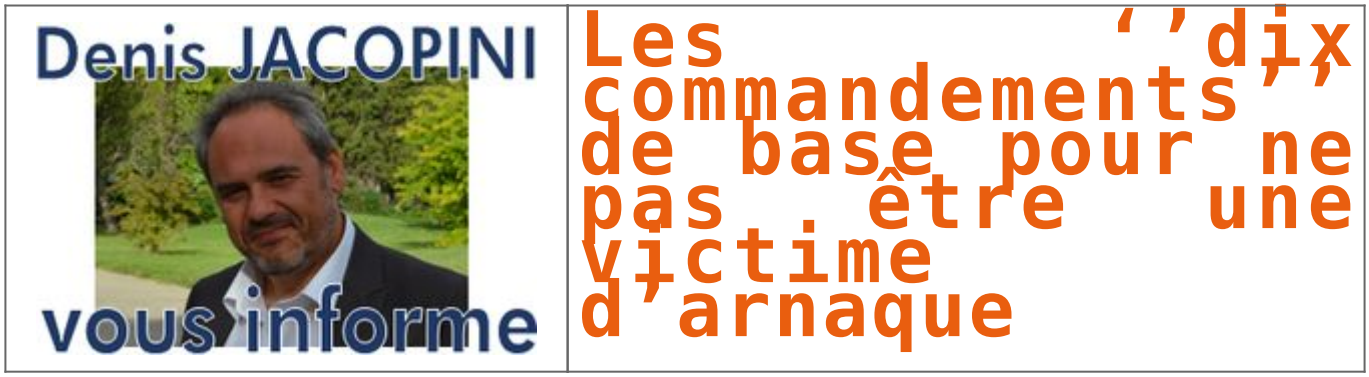
Sources :

IT-Forum 2016 – 8e édition du Forum des décideurs et acteurs des Technologies de l'Information

http://it-forum.ci

https://www.eventbrite.fr/e/inscription-it-forum-2016-8eme-edition-24951266911

Les ‘’dix commandements’’ de base pour ne pas être une victime d'arnaque



Les cybercriminels continuent de faire de nombreuses victimes à travers le monde. Si des moyens de répression de cette activité criminelle sont entrepris dans nos différents pays, l'un des moyens les plus efficaces de l'éradiquer reste la prévention.

Dans cet article, la Plateforme de lutte contre la cybercriminalité (PLCC) fait un rappel en 10 points des mesures à prendre pour naviguer sur la toile en toute sécurité.

1- Changer régulièrement vos mots de passe. (Un site = Un mot de passe unique)

2- Aucune autorité judiciaire, de police ne possède d'adresse mail gratuite de type Hotmail, Yahoo, Gmail…

3- Ne divulguez pas d'informations personnelles sur Internet. Prenez le temps de sécuriser vos comptes ainsi que ceux de vos enfants. Ne rendez pas visibles vos contacts sur Facebook ou autre réseau sociale.

4- Allez toujours sur une adresse commençant par https://, officielle et habituelle pour vous connecter à votre compte bancaire, à votre messagerie ou autres réseaux sociaux.

5- Evitez d'envoyer des photos ou vidéos, de vous, à caractère sexuelle ou tout autre position indélicate.

6- Ne versez jamais d'argent par Mandat Cash ou Western Union à une personne que vous ne connaissez pas, que vous n'avez jamais rencontrée physiquement.

7- Méfiez-vous des trop bonnes affaires. Ne cédez jamais à la précipitation. Les bases d'une transaction sont les mêmes dans la réalité et sur Internet. Une annonce trop alléchante cache souvent une arnaque. Renseignez-vous, comparez les prix et les produits avant d'acheter.

8- Cessez tout contact si votre interlocuteur (que vous ne connaissez pas) vous demande de l'argent sous prétexte de frais, de maladie, de transport…

9- Remettez vous souvent en question. Il n'y a pas de profil type de victime, personne n'est à l'abri sur Internet. Les cyberdélinquants jouent parfois sur notre confiance excessive en nos capacités.

10- Ayez un anti-virus efficace et à jour sur votre ordinateur.

Une fois de plus, la PLCC vous exhorte à la prudence !… [Lire la suite]

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet…) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Source : *Lutte contre la cybercriminalité: Voici les ‘’dix commandements’’ de base pour ne pas être une victime d’arnaque*

RGPG Règlement européen sur la protection des données : priorité au chiffrement, à l’authentification et aux contrôles d’accès

	**RGPD : Règlement européen sur la protection des données : priorité au chiffrement, à l’authentification et aux contrôles d’accès**

Philippe Carrère, directeur de la protection des données et de l'identité, Europe du Sud chez Gemalto revient sur le nouveau règlement européen sur la protection des données personnelles et ce qu'il implique pour les entreprises en termes de stratégie de sécurité et de relation client.

L'adoption récente du règlement européen sur la protection des données personnelles constitue un tournant pour les entreprises implantées dans l'Union Européenne. En effet, il exige des gestionnaires d'infrastructures et des fournisseurs de services numériques – tels qu'Amazon ou Google – de faire part d'éventuels vols de données et de mettre en place des mesures de sécurité adéquates. Les chefs d'entreprises devraient y voir là un avertissement et commencer dès à présent à évaluer leurs politiques de sécurité, avant que la proposition de loi ne soit approuvée par le Parlement et le Conseil européen.
Où en sont les entreprises européennes en termes de sécurité des données et quelles mesures doivent-elles prendre afin d'être conformes ? A l'heure actuelle, les pare-feu, les antivirus, le filtrage de contenu et la détection des menaces sont les principaux outils utilisés pour se prémunir des vols de données. Ces mesures sont, cependant, insuffisantes, les hackers pouvant franchir aisément ce premier périmètre de sécurité. Dès lors, l'adresse IP des entreprises ou encore les informations de leurs clients peuvent être compromises, comme ce fut le cas avec Volkswagen et la conception de sa Passat.
D'après le Breach Level Index réalisé pour l'année 2015 par Gemalto, plus de 707,5 millions de dossiers clients ont été volés ou perdus à la suite de 1 673 cyberattaques menées de par le monde. Un chiffre qui devrait faire l'effet d'un véritable électrochoc pour les responsables informatiques, d'autant que, fait encore plus inquiétant, 4 % des infractions ont impliqué des données sécurisées (chiffrées partiellement ou en totalité).
Les clients confient des données confidentielles, et ils doivent donc être assurés et convaincus de leur sécurité. Si le lien de confiance avec le client vient à être brisé, il peut être très difficile pour les entreprises de le renouer.
Une de nos récentes études a révélé que plus de la moitié des individus interrogés (57 %) ne traiterait jamais, ou très peu probablement, avec une société ayant perdu des données personnelles suite à une cyberattaque.

Pourquoi ce règlement apparaît aujourd'hui comme une nécessité ?
La sécurité a toujours été un sujet d'actualité, mais suite aux récentes attaques, comme celle de Talk Talk, et le fait que de plus en plus de données personnelles sont collectées en ligne, assurer leur sécurité et maintenir une relation de confiance avec les clients n'a jamais été aussi primordial. A l'heure actuelle, les entreprises européennes ne sont pas tenues de signaler les brèches de données dont elles peuvent faire l'objet, et, de fait, grand nombre d'entre elles ne le font pas. Une fois la nouvelle réglementation en vigueur, elles seront dans l'obligation de révéler ces violations, sous peine de se voir infliger une amende pouvant aller jusqu'à 4 % de leur chiffre d'affaires. C'est pourquoi elles doivent dès à présent opérer un changement de stratégie.
Cependant, il ne s'agit pas là d'un fait nouveau. Cette pratique est déjà en place depuis plusieurs années aux Etats-Unis. C'est pourquoi nous entendons davantage parler des cyberattaques ayant lieu outre-Atlantique que celles se produisant près de chez nous.

Quels sont les principaux enseignements à en tirer ?
Au lieu de se concentrer uniquement sur la protection du périmètre de sécurité, les entreprises devraient plutôt adopter une approche segmentée, protégeant les données à tous les niveaux et barrant le passage aux hackers qui auraient franchi le 1er palier de défense. Cela signifie également que la priorité doit porter sur les données elles-mêmes et sur le fait qu'elles ne puissent être consultées ou utilisées par des personnes non autorisées. Protéger les données par des solutions de chiffrement de bout en bout, d'authentification et des contrôles d'accès permet d'ajouter un niveau de sécurité supplémentaire. En mettant en place des outils de chiffrement, les données subtilisées n'ont plus aucune valeur pour toute personne non autorisée. L'accès peut être sécurisé en utilisant des clés permettant aux personnes habilitées de consulter les informations. Ainsi, en cas d'attaque, les entreprises sont certaines de garantir la sécurité des données de leurs clients.

Informer les clients
Une fois ces mesures sécuritaires mises en place, il est important d'en informer les clients et de les rassurer quant à la pertinence des processus instaurés pour protéger leurs données. Si les entreprises peuvent démontrer qu'elles sont prêtes à se dépasser et à mettre toute leur énergie dans cette démarche, elles seront perçues comme innovantes et dignes de confiance.
La sécurité est un effort mutuel. S'il est important d'informer les clients sur le travail qui est fait pour assurer leur sécurité, il est tout aussi primordial qu'ils sachent comment se protéger eux-mêmes. De plus, s'adresser à un utilisateur averti permettra de lui proposer un meilleur service client.
L'adoption du nouveau règlement européen sur la protection des données donne aux entreprises la possibilité de prendre les devants et montrer dès à présent à leurs clients qu'elles prennent ce sujet très au sérieux. Elles ne doivent pas seulement se soucier d'être conformes ou pas, mais comprendre qu'il s'agit là d'une nécessité essentielle à leur réussite. Les utilisateurs sont de plus en plus conscients qu'ils confient des données sensibles aux entreprises, leur demandant, de fait, d'en être responsables. La montée en puissance de cette prise de conscience doit aller de pair avec un niveau d'exigence plus élevé vis-à-vis des structures hébergeant ces informations. Ne pas prendre ce sujet au sérieux pourrait non seulement être préjudiciable en cas d'attaque, mais également nuire à la confiance instaurée avec les clients. Perdre ce lien les incitera à se tourner vers des concurrents jugés plus fiables… [Lire la suite]

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Source : *Nouveau règlement européen sur la protection des données : priorité au chiffrement, à l'authentification et aux contrôles d'accès | Solutions Numériques*

Paypal ne protégera plus les transactions crowdfunding

	**Paypal ne protégera plus les transactions crowdfunding**

Trop d'arnaques au financement participatif ? Trop de remboursements pour des produits jamais livrés ? Paypal ne protégera plus les transactions crowdfunding à partir de la fin juin 2016.

Paypal semble ne plus apprécier les transactions bancaires entre ses utilisateurs et les projets lancés sur les portails de crowdfunding. Trop d'arnaques au Crowdfunding ? Á partir du 26 juin 2016, le géant de la finance, ne protégera plus les transactions effectuées sur les sites de financement participatif.
Trop d'arnaques au transactions crowdfunding ? Trop d'argent envolé sans le moindre produit/projet finalisé ? Bref, des problèmes se posent des deux côtés – vendeurs et acheteurs. Paypal ne veut tout simplement plus faire partie d'une équation qui le place au milieu des conflits. Par conséquent, vous pourrez toujours payer via Paypal, mais la structure financière n'assurera plus cette transaction. Elle sera à vos risques et périls.

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Source : *ZATAZ Paypal ne protégera plus les transactions crowdfunding – ZATAZ*

Liberté de la presse en Ukraine: journaliste = terroriste?

Liberté de la presse en Ukraine: journaliste = terroriste?

Alors que le métier des journalistes travaillant dans des zones sensibles reste difficile et dangereux, le site ukrainien Mirotvorets soutenu par le député ukrainien Anton Guerachtchenko, conseiller du ministre de l'Intérieur, les compare à des « terroristes accrédités ». Une comparaison qui n'a pas manqué de semer le malaise.

Sputnik a recueilli les propos d'une des journalistes faisant partie de la liste, à savoir d'Anne Nivat, politologue, journaliste et écrivaine française auteure de plusieurs livres, spécialisée depuis près de seize ans dans des zones sensibles, dont la Tchétchénie, l'Irak, l'Afghanistan etc., parfois même clandestinement.
« Traiter ces journalistes — dont je fais partie — de « complices de terroristes » est une ineptie qui, pour moi, n'a aucun sens », a déclaré Mme Nivat dans une interview à Sputnik.
Et d'ajouter: « En tant que reporter de guerre couvrant depuis près de 20 ans des zones de conflit (Balkans, Tchétchénie, Asie centrale, Irak, Syrie et Afghanistan) en toute indépendance, je continuerai à le faire y compris en Ukraine, cela va sans dire ».

Liberté de la presse: l' »Ukraine tend à ressembler à la Turquie »
Cette opinion de la journaliste est étayée par le Pacte onusien sur les droits civils et politiques, ou la Convention européenne des droits de l'Homme, selon laquelle les travailleurs des médias ne devraient pas être poursuivis pour l'exercice de leurs fonctions professionnelles.

Le Conseil de l'Europe accuse Kiev et Ankara d'intimider les médias
Un des points les plus problématiques est que la publication des noms des journalistes pourrait être lourde de conséquences, car leur sécurité est mise en question: c'est juste après la publication des données personnelles d'Oles Bouzina par le site Mirotvorets que le journaliste ukrainien avait été assassiné.
Selon la porte-parole de l'Organisation pour la sécurité et la coopération en Europe (OSCE) pour la liberté des médias Dunja Mijatovic, certains journalistes de la liste ont déjà commencé à recevoir des menaces.
S'étant fixé pour objectif de lutter contre les « ennemis de l'Ukraine », le site ukrainien Mirotvorets (« le faiseur de paix » en ukrainien) a publié les données personnelles (numéro de téléphone, e-mail, nom du service de presse) de milliers de journalistes, dont une cinquantaine de Français et un millier d'occidentaux.
Toutes sortes d'agences de presse sont concernées, de toutes nationalités: CNN, ABC, Al-Jazeera, AFP, Reuters, RT, ZDF, RTL, Europe 1… [Lire la suite]

Réagissez à cet article

Source : *Liberté de la presse en Ukraine: journaliste = terroriste?*

Combien vous coûterait le piratage de vos données ?

	Combien vous coûterait le piratage de vos données ?

Un consommateur français sur trois reconnaît que sa loyauté envers une marque diminue après qu'une attaque informatique a porté atteinte aux données qu'il lui avait confié.

Souvent préparées de longues dates, les attaques informatiques qui frappent les entreprises laissent des traces longtemps après.
Publiée aujourd'hui, une étude internationale menée par Vanson Bourne, pour l'éditeur de logiciels de cybersécurité FireEye, souligne que les conséquences de tels épisodes entament la performance commerciale de la société victime, au-delà des dégâts informatiques des premiers jours. « *La sécurité des systèmes d'information a un réel impact sur la confiance des consommateurs* », affirme Yogi Chandiramani, directeur des ventes en Europe pour FireEye.
« *En France, l'attaque qui a touché TV5 Monde en avril 2015 et les vols de données chez Orange en 2014 ont particulièrement marqué les esprits* », poursuit-il. 34 % des consommateurs français reconnaissent que leur loyauté en tant que client actuel ou potentiel d'une marque diminue après qu'une entreprise a laissé fuiter des données, pointe le questionnaire en ligne envoyé à 1.000 d'entre eux. Un argument de plus pour ceux qui voient les efforts de cyber-sécurité comme un argument de compétitivité .
L'atteinte à leurs données personnelles refroidit particulièrement les ardeurs à l'achat des consommateurs. Quand le vol de données est connu, plus de trois Français sur quatre déclarent qu'ils stopperaient leurs emplettes de produits ou services fournis par la victime, surtout si la faute vient de l'équipe dirigeante – ils sont plus conciliants s'il s'agit de l'erreur humaine d'un subordonné. La tendance se confirme au fil des années. D'après l'étude, 61 % des Français déclarent avoir pris en considération la sécurité de leurs données lors de leurs achats en 2015. Ils n'étaient que 53% dans cet état d'esprit en 2014…

Après une cyber-attaque, la transparence prime

A cette perte de chiffre d'affaires potentiel s'ajoute le risque de poursuite en justice. La moitié des Français déclarent qu'ils engageraient des poursuites contre l'entreprise cyber-attaquée qui n'a pas su protéger leurs données personnelles, volées ou utilisées à des fins criminelles. Aux Etats-Unis, Target et Sony Picture s ont été attaqués en Justice par des procédures de class action, le premier par ses clients, le second par ses salariés.
Dès lors, la tentation peut être grande pour une entreprise de garder secret le fait que son système d'information ait été vulnérable à des cyber-criminels. Ce serait pourtant aggraver le mal qui surviendra au moment où, inévitablement à l'heure d'Internet, l'information ressortira.
« *Les consommateurs pointent les négligences des entreprises mais attendent surtout d'elles de la transparence, 93 % d'entre eux souhaitent être prévenus dans les 24h quand leurs données sont exposées* », prévient Yogi Chandiramani.

Des changements dans quelques mois ?

Le règlement européen sur la protection des données, qui devrait s'appliquer en France d'ici 2018, prévoit d'imposer aux sociétés de notifier les autorités, voir leurs clients, de toutes atteintes sur les données personnelles des citoyens européens dans les 72h après la découverte du problème.
A noter :
L'attaque particulièrement destructrice qui a touché TV5Monde en 2015 devrait coûter près de 10 millions d'euros sur trois ans, uniquement en réparation informatique… [Lire la suite]

Réagissez à cet article

Source : *Cyber-attaque : les coûts d'après, Cybersécurité – Les Echos Business*

La police peut-elle obliger un suspect à débloquer son iPhone avec son doigt ?

La police peut-elle obliger un suspect à débloquer son iPhone avec son doigt ?

Aux États-Unis, une affaire judiciaire pose la question du droit que peuvent avoir les autorités judiciaires à contraindre un suspect à débloquer son iPhone avec le capteur Touch ID qui permet d'accéder au contenu du téléphone avec les empreintes digitales.

La question s'est certainement déjà posée dans les commissariats et dans les bureaux des juges d'instruction, et elle devrait devenir plus pressant encore dans les années à venir : alors qu'un suspect peut toujours prétendre avoir oublié son mot de passe, ou refuser de répondre, les enquêteurs peuvent-ils contraindre un individu à débloquer son téléphone lorsque celui-ci est déblocable avec une simple empreinte digitale ?
Le débat sera tranché aux États-Unis par un tribunal de Los Angeles. Le Los Angeles Times rapporte en effet qu'un juge a délivré un mandat de perquisition à des policiers, qui leur donne le pouvoir de contraindre physiquement la petite amie d'un membre d'un gang arménien à mettre son doigt sur le capteur Touch ID de son iPhone, pour en débloquer le contenu.

Le mandat signé 45 minutes après son placement en détention provisoire a été mis en œuvre dans les heures qui ont suivi. Le temps était très court, peut-être en raison de l'urgence du dossier lui-même, mais aussi car l'iPhone dispose d'une sécurité qui fait qu'au bout de 48 heures sans être débloqué, il n'est plus possible d'utiliser l'empreinte digitale pour accéder aux données. Mais l'admissibilité des preuves ainsi collectées reste sujette à caution et fait l'objet d'un débat entre juristes.

EN MONTRANT QUE VOUS AVEZ OUVERT LE TÉLÉPHONE, VOUS DÉMONTREZ QUE VOUS AVEZ CONTRÔLE SUR LUI
Certains considèrent qu'obliger un individu à placer son doigt sur le capteur d'empreintes digitales de son iPhone pour y gagner l'accès revient à forcer cette personne à fournir elle-même les éléments de sa propre incrimination, ce qui est contraire à la Constitution américaine et aux traités internationaux de protection des droits de l'homme. « En montrant que vous avez ouvert le téléphone, vous montrez que vous avez contrôle sur lui », estime ainsi Susan Brenner, une professeur de droit de l'Université de Dayton. Le capteur Touch ID ne sert pas uniquement à débloquer le téléphone, mais aussi à le déchiffrer, en fournissant une clé qui joue le rôle d'authentifiant du contenu.
D'autres estiment qu'il s'agit ni plus ou moins que la même chose qu'une perquisition à domicile réalisée en utilisant la clé portée sur lui par le suspect, ce qui est chose courante et ne fait pas l'objet de protestations. Ils n'y voient pas non plus de violation du droit de garder le silence, puisque le suspect ne parle pas en ne faisant que poser son doigt sur un capteur.

ET EN FRANCE ?
Pour le moment, le sujet n'est pas venu sur la scène législative en France. Mais il pourrait y venir par analogie avec d'autres techniques d'identification biométrique.
En matière de recherche d'empreintes digitales ou de prélèvement de cheveux pour comparaison, l'article 55-1 du code de procédure pénale punit d'un an de prison et 15 000 euros d'amende « le refus, par une personne à l'encontre de laquelle il existe une ou plusieurs raisons plausibles de soupçonner qu'elle a commis ou tenté de commettre une infraction, de se soumettre aux opérations de prélèvement ». De même en matière de prélèvements ADN, le code de procédure pénale autorise les policiers à exiger qu'un prélèvement biologique soit effectué sur un suspect, et « le fait de refuser de se soumettre au prélèvement biologique est puni d'un an d'emprisonnement et 30 000 euros d'amende ».
Sans loi spécifique, les policiers peuvent aussi tenter de se reposer sur les dispositions anti-chiffrement du code pénal, puisque l'empreinte digitale sert de clé. L'article 434-15-2 du code pénal punit de 3 ans de prison et 45 000 euros d'amende le fait, « pour quiconque ayant connaissance de la convention secrète de déchiffrement d'un moyen de cryptologie susceptible d'avoir été utilisé pour préparer, faciliter ou commettre un crime ou un délit, de refuser de remettre ladite convention aux autorités judiciaires ou de la mettre en oeuvre, sur les réquisitions de ces autorités ». Mais à notre connaissance, elle n'a jamais été appliquée pour forcer un suspect à fournir lui-même ses clés de chiffrement, ce qui serait potentiellement contraire aux conventions de protection des droits de l'homme… [Lire la suite]

Réagissez à cet article

Source : *La police peut-elle obliger un suspect à débloquer son iPhone avec son doigt ? – Politique – Numerama*